

Secrecy Capacity Optimization in Coordinated Multi-Point Processing

Meng Zhang, Ruiqi Xue, Hui Yu, Hanwen Luo and Wen Chen
 Depart. of Electronic Engineering, Shanghai Jiao Tong University, China
 Email: {mengzhang, xrq, yuhui, hwluo, wenchen}@sjtu.edu.cn

Abstract—¹In this paper, we will consider a coordinated multi-point (CoMP) transmission system which accords with the current Long Term Evolution-Advanced (LTE-A) system and the 5th generation wireless system (5G). This paper will consider two different circumstances, one concerning the condition that transmitters know exactly which user will be wiretapped; the other concerning the condition that transmitters have no knowledge about the wiretapped user's index. Accordingly, we provide the corresponding precoding strategies and simulation results to verify the effectiveness of our proposed algorithms.

I. INTRODUCTION

Although primitive concept about secrecy transmission was proposed by Shannon in 1940s [1], secrecy issues concerning wireless transmission have drawn considerable attention in recent years. Wyner shows how to guarantee a secure communication for the case that the intended receiver has a better channel condition than the eavesdropper's [2]. Nevertheless, for a long time researchers resort to cryptographic algorithm to ensure secures transmissions. Such kind of cryptographic algorithms usually base on pre-established protocols among distinct parties. However, it often neglects taking the power loss and complexity into account. Besides, such kinds of protocol are difficult to be realized in wireless local area networks (WLAN) or device-to-device (D2D) communications since one might access and leave randomly. In addition, wireless transmission is vulnerable to exterior attacks in these situations due to the broadcast nature of wireless communications.

With the developments of multiple antennas technology, physical layer security has been proposed to realize secure communications which is mainly defined as the difference between the capacity achieved by the eavesdropper and its wiretapped user's. Broadly speaking, the physical layer security can be classified into two categories, one is based on precoding technology, and the other is based on adding artificial noise. In [3], the author studies a relay assisted system with the assumption that the relay is unreliable. Precoding designs of the base station and relay, which can maximize the secrecy capacity, are provided in this paper. In [4] and [5], the authors analyze enhancing secrecy capacity with aid of artificial noise. The difference is that in [4] the artificial noise is generated by the transmitter, while in [5] there exists an external helper to accomplish this work.

¹This paper is partially sponsored by Shanghai Basic Research Key Project (No.11DZ1500206) and National Key Project of China (No.2012ZX03001013-003), and by the National 973 Project #2012CB316106 and NSF China #61161130529.

This paper will consider a coordinated multi-point transmission scenario where there exist multiple base stations and multiple users. As well known, CoMP has become a core technology for the Long Term Evolution-Advanced (LTE-A) system and will be continuously enhanced in the 5G. In our model, we assume that each base station will serve one specific user and CSIs are collected by a central processor. Additionally, there exists one eavesdropper who will wiretap one of the users. However, the transmitters might not know exactly which user will be wiretapped, thus the transmitting strategies will vary according to the distinct status of pre-known knowledge at transmitter side. To our best knowledge, it is the first time that someone launches studies under such assumptions.

The rest of the paper is organized as follows. The system model and problem formulation are described in section II. The joint precoding design with pre-known wiretapping knowledge is proposed in section III. Similarly, we discuss joint precoding design without pre-known wiretapping knowledge in section IV. The numerical results are presented in section V. Finally, the conclusion is made in section VI.

Notation: In this paper, we use bold uppercase and lowercase letters denote matrices and vectors, respectively; $(\cdot)^T$, $(\cdot)^H$, denote the conjugate, transpose, conjugate transpose and inverses of a matrix or a vector, respectively; $\text{blkdiag}\{\mathbf{X}_1, \mathbf{X}_2, \dots, \mathbf{X}_N\}$ is the block diagonalized matrix formed by matrices $\mathbf{X}_i, i = 1, 2, \dots, N$; \mathbf{I}_N is an $N \times N$ identity matrix; $\text{Tr}(\cdot)$ is the trace of a matrix; $\text{vec}(\cdot)$ represents the matrix vectorization;; \otimes denotes the Kronecker product; $\|\cdot\|$ denotes the Frobenius norm; \succeq represents the property of semidefinite.

II. SYSTEM MODEL AND PROBLEM FORMULATION

In this paper, we study a multi-cell scenario incorporating K base stations which function under the same time-frequency resource. Each cell is assigned with single base station and single user. There exists one eavesdropper in the system whose objective is to wiretap the message intended for a specific user. We assume that each base station serves one particular user situated in the same cell and it only possesses the specific user's intended message. Besides, it is also assumed that there exists a central processor whose role is to collect all the CSI including the eavesdropper's and computes the appropriate precoders that can maximize the system performance. For ease

of discussion, we assume that the k -th base station and the k -th user equips the same N_k antennas. The eavesdropper is assumed to equip N_e antennas. Therefore, the received signal at k -th user can be expressed as

$$\mathbf{y}_i = \sum_{k=1}^K \mathbf{H}_{ik} \mathbf{F}_k \mathbf{s}_k + \mathbf{n}_i, \quad (1)$$

where $\mathbf{H}_{ik} \in \mathbb{C}^{N_i \times N_k}$ denotes the channel between the k -th base station and the i -th user; $\mathbf{F}_k \in \mathbb{C}^{N_k \times N_k}$ is the precoding matrix executed at the k -th base station; $\mathbf{s}_k \in \mathbb{C}^{N_k \times 1}$ is the vector intended for the k -th user with covariance $\sigma_s^2 \mathbf{I}$; $\mathbf{n}_i \in \mathbb{C}^{N_i \times 1}$ is the white Gaussian noise vector with covariance $\sigma_i^2 \mathbf{I}$ experienced at the i -th user. Similarly, the received signal at the eavesdropper can be written as

$$\mathbf{y}_e = \sum_{k=1}^K \mathbf{H}_{ek} \mathbf{F}_k \mathbf{s}_k + \mathbf{n}_e, \quad (2)$$

where $\mathbf{H}_{ek} \in \mathbb{C}^{N_e \times N_k}$ is the channel between the eavesdropper and the k -th base station and $\mathbf{n}_e \in \mathbb{C}^{N_e \times 1}$ denotes the white Gaussian noise vector with covariance $\sigma_e^2 \mathbf{I}$ experienced at the eavesdropper. In this paper, we have individual power constraints for all base stations, which is

$$\text{Tr}(\mathbf{F}_k \mathbf{F}_k^H) \leq P_k, k = 1, 2, \dots, K, \quad (3)$$

The i -th user's signal to interference plus noise ratio (SINR) can be defined as

$$\text{SINR}_i = \frac{\|\mathbf{H}_{ii} \mathbf{F}_i\|^2}{\sum_{k=1, k \neq i}^K \|\mathbf{H}_{ik} \mathbf{F}_k\|^2 + N_i \sigma_i^2}. \quad (4)$$

We denote the w -th user as the user that has been wiretapped. Accordingly, the wiretapped user's SINR can be written as

$$\text{SINR}_w = \frac{\|\mathbf{H}_{ww} \mathbf{F}_w\|^2}{\sum_{k=1, k \neq w}^K \|\mathbf{H}_{wk} \mathbf{F}_k\|^2 + N_w \sigma_w^2}. \quad (5)$$

Similarly, we could express the eavesdropper's SINR as

$$\text{SINR}_e = \frac{\|\mathbf{H}_{ek} \mathbf{F}_k\|^2}{\sum_{k=1, k \neq w}^K \|\mathbf{H}_{ek} \mathbf{F}_k\|^2 + N_e \sigma_e^2}. \quad (6)$$

Based on the above expressions, we can define the secrecy capacity as

$$\mathcal{C} = |\mathcal{C}_w - \mathcal{C}_e|^\dagger, \quad (7)$$

where $\mathcal{C}_w = \log(1 + \text{SINR}_w)$ and $\mathcal{C}_e = \log(1 + \text{SINR}_e)$ denote the capacity achieved by the wiretapped user and the eavesdropper, respectively; $|x|^\dagger$ denotes $\max\{x, 0\}$.

In this paper, we will discuss two different scenarios classified according to distinct pre-known wiretapping knowledge at the transmitter side. In the first scenario, we assume that all channel state information (CSI) involving the eavesdropper's is known at the transmitter side. Furthermore, we also know which user will be wiretapped. In the second scenario, although we can still access all CSI, we do not know the wiretapped user's index. Then in the following two sections, we will propose our joint precoding design according to the two scenarios, respectively.

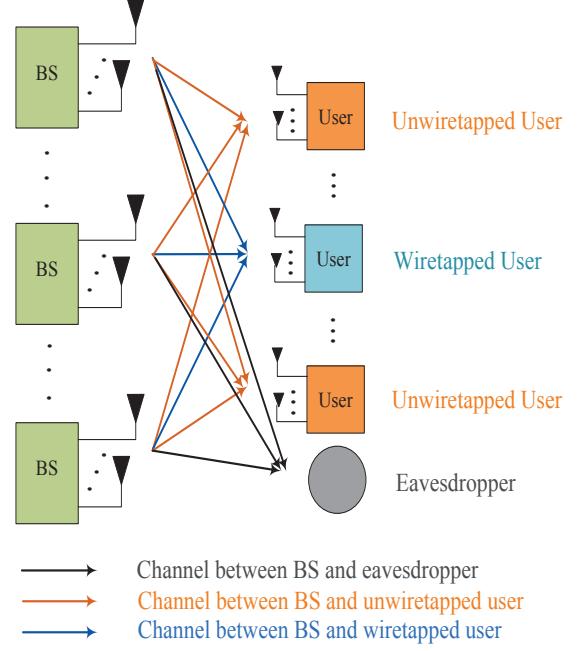


Fig. 1. Illustration of wiretapping model

III. JOINT PRECODING DESIGN WITH PRE-KNOWN WIRETAPPING KNOWLEDGE

Although it is more preferable to directly optimize the secrecy capacity in (7), it is a very difficult task due to the non-convex nature of the expression \mathcal{C} . Therefore, we resort to optimizing \mathcal{C}_w and \mathcal{C}_e independently. Since \mathcal{C}_w and \mathcal{C}_e are related to SINR_w and SINR_e , we will turn to optimize SINR_w and SINR_e instead.

In this section, we will discuss the case with hypothesis that all CSI and the wiretapped user's index are pre-known at the transmitter sides. Due to the fact that we have already known which user will be wiretapped, we are capable of expressing the capacity achieved by eavesdropper. Therefore, in order to optimize the secrecy capacity, we maximize the capacity of wiretapped user while maintaining the eavesdropper's capacity below certain threshold. Besides, we do not want that our optimization method will degrade the capacity of other unwiretapped users. Naturally, we also should guarantee the other user's SINR above certain thresholds. Our optimization problem can be formulated as follows

$$\max_{\mathbf{F}_k, k \in \{1, 2, \dots, K\}} \text{SINR}_w, \quad (8a)$$

$$\text{s.t. } \text{Tr}(\mathbf{F}_k \mathbf{F}_k^H) \leq P_k, k = 1, 2, \dots, K, \quad (8b)$$

$$\text{SINR}_e \leq r_e \quad (8c)$$

$$\text{SINR}_i \geq r_i, i = 1, 2, \dots, K, i \neq k, \bar{k} \quad (8d)$$

Inserting (4) (5) and (6) into (8), we get the following

expressions

$$\max_{\mathbf{F}_k, k \in \{1, 2, \dots, K\}} \frac{\|\mathbf{H}_{ww}\mathbf{F}_w\|^2}{\sum_{k=1, k \neq w}^K \|\mathbf{H}_{wk}\mathbf{F}_k\|^2 + N_w\sigma_w^2}, \quad (9a)$$

$$s.t. \quad Tr(\mathbf{F}_k\mathbf{F}_k^H) \leq P_k, \quad k = 1, 2, \dots, K, \quad (9b)$$

$$\frac{\|\mathbf{H}_{ew}\mathbf{F}_w\|^2}{\sum_{k=1, k \neq w}^K \|\mathbf{H}_{ek}\mathbf{F}_k\|^2 + N_e\sigma_e^2} \leq r_e, \quad (9c)$$

$$\frac{\|\mathbf{H}_{ii}\mathbf{F}_i\|^2}{\sum_{k=1, k \neq i}^K \|\mathbf{H}_{ik}\mathbf{F}_k\|^2 + N_i\sigma_i^2} \geq r_i, \quad i = 1, 2, \dots, K, i \neq w, \quad (9d)$$

where r_e and r_i denote the thresholds for eavesdropper and unwiretapped user, respectively.

In traditional coordinated precoding design [6], people might tend to optimize $\mathbf{F}_k, k \in \{1, 2, \dots, K\}$ iteratively. Although such method is easy to implement, it can not ensure a global optimal solution since this algorithm usually leads to an iterative solution that needs to optimize \mathbf{F}_k successively. However, it is more preferable to optimize all the precoders simultaneously so as to avoid a local optimal solution. Therefore, we utilize the technique introduced in [7]. First, we define $\mathbf{F} = blkdiag\{\mathbf{F}_1, \mathbf{F}_2, \dots, \mathbf{F}_K\}$. Then, it is easy to verify that $\mathbf{F}_r = \mathbf{P}_r \mathbf{F} \mathbf{P}_r^T$, where \mathbf{P}_r is the $N_k \times \sum_{r=1}^K N_r$ permutation matrix with zeros and ones.

Introduce the equation $vec(\mathbf{F}) = \mathbf{T}_f \mathbf{f}$, where $\mathbf{f} = [vec(\mathbf{F}_1), \dots, vec(\mathbf{F}_R)]^T$. \mathbf{T}_f is the transformation matrix formed by ones and zeros, which can be built by observing the nonzero entries of $vec(\mathbf{F})$. Thus, with the help of equations $Tr(\mathbf{X}^H \mathbf{Y} \mathbf{X} \mathbf{W}) = vec(\mathbf{X})^H (\mathbf{W}^T \otimes \mathbf{Y}) vec(\mathbf{X})$ and $Tr(\mathbf{A}\mathbf{B}) = Tr(\mathbf{B}\mathbf{A})$ [8], (9a) can be rewritten as

$$\frac{\|\mathbf{H}_{ww}\mathbf{F}_w\|^2}{\sum_{k=1, k \neq w}^K \|\mathbf{H}_{wk}\mathbf{F}_k\|^2 + N_w\sigma_w^2} = \frac{Tr(\mathbf{A}\mathbf{f}\mathbf{f}^H)}{Tr(\mathbf{B}\mathbf{f}\mathbf{f}^H) + N_w\sigma_w^2}, \quad (10)$$

where

$$\mathbf{A} = \mathbf{T}_f^H \left((\mathbf{P}_w^T \mathbf{P}_w)^T \otimes (\mathbf{P}_w^T \mathbf{H}_{ww}^H \mathbf{H}_{ww} \mathbf{P}_w) \right) \mathbf{T}_f, \quad (11)$$

$$\mathbf{B} = \sum_{k=1, k \neq w}^K \mathbf{T}_f^H \left((\mathbf{P}_k^T \mathbf{P}_k)^T \otimes (\mathbf{P}_k^T \mathbf{H}_{wk}^H \mathbf{H}_{wk} \mathbf{P}_k) \right) \mathbf{T}_f. \quad (12)$$

Similarly, the constraints of (9c) and (9d) can also be turned into

$$\frac{\|\mathbf{H}_{ew}\mathbf{F}_w\|^2}{\sum_{k=1, k \neq w}^K \|\mathbf{H}_{ek}\mathbf{F}_k\|^2 + N_e\sigma_e^2} = \frac{Tr(\mathbf{C}\mathbf{f}\mathbf{f}^H)}{Tr(\mathbf{D}\mathbf{f}\mathbf{f}^H) + N_w\sigma_w^2}, \quad (13)$$

$$\frac{\|\mathbf{H}_{ii}\mathbf{F}_i\|^2}{\sum_{k=1, k \neq i}^K \|\mathbf{H}_{ik}\mathbf{F}_k\|^2 + N_i\sigma_i^2} = \frac{Tr(\mathbf{E}_i\mathbf{f}\mathbf{f}^H)}{Tr(\mathbf{M}_i\mathbf{f}\mathbf{f}^H) + N_i\sigma_i^2}, \quad (14)$$

where

$$\mathbf{C} = \mathbf{T}_f^H \left((\mathbf{P}_w^T \mathbf{P}_w)^T \otimes (\mathbf{P}_w^T \mathbf{H}_{ew}^H \mathbf{H}_{ew} \mathbf{P}_w) \right) \mathbf{T}_f, \quad (15)$$

$$\mathbf{D} = \sum_{k=1, k \neq w}^K \mathbf{T}_f^H \left((\mathbf{P}_k^T \mathbf{P}_k)^T \otimes (\mathbf{P}_k^T \mathbf{H}_{ek}^H \mathbf{H}_{ek} \mathbf{P}_k) \right) \mathbf{T}_f, \quad (16)$$

$$\mathbf{E}_i = \mathbf{T}_f^H \left((\mathbf{P}_i^T \mathbf{P}_i)^T \otimes (\mathbf{P}_i^T \mathbf{H}_{ii}^H \mathbf{H}_{ii} \mathbf{P}_i) \right) \mathbf{T}_f, \quad (17)$$

$$\mathbf{M}_i = \sum_{k=1, k \neq i}^K \mathbf{T}_f^H \left((\mathbf{P}_k^T \mathbf{P}_k)^T \otimes (\mathbf{P}_k^T \mathbf{H}_{ik}^H \mathbf{H}_{ik} \mathbf{P}_k) \right) \mathbf{T}_f, \quad (18)$$

The power constraints are equivalent to

$$Tr(\mathbf{F}_k\mathbf{F}_k^H) = Tr(\mathbf{N}_k\mathbf{f}\mathbf{f}^H), \quad \forall k \in \{1, 2, 3, \dots, K\}, \quad (19)$$

where

$$\mathbf{N}_k = \mathbf{T}_f^H \left((\mathbf{P}_k^T \mathbf{P}_k)^T \otimes (\mathbf{P}_k^T \mathbf{P}_k) \right) \mathbf{T}_f. \quad (20)$$

Additionally, after the above processing, the problem in (9) is still nonconvex [9]. To make the problem more tractable, we introduce a new matrix $\mathbf{W} = \mathbf{f}\mathbf{f}^H$. Therefore, the optimization problem can be reformulated as

$$\max_{\mathbf{W}} \frac{Tr(\mathbf{AW})}{Tr(\mathbf{BW}) + N_i\sigma_i^2}, \quad (21a)$$

$$s.t. \quad Tr(\mathbf{N}_k\mathbf{W}) \leq P_k, \quad k = 1, 2, \dots, K, \quad (21b)$$

$$\frac{Tr(\mathbf{CW})}{Tr(\mathbf{DW}) + N_w\sigma_w^2} \leq r_e, \quad (21c)$$

$$\frac{Tr(\mathbf{E}_i\mathbf{W})}{Tr(\mathbf{M}_i\mathbf{W}) + N_i\sigma_i^2} \geq r_i, \quad i = 1, 2, \dots, K, i \neq w, \quad (21d)$$

$$\mathbf{W} \succeq 0, rank(\mathbf{W}) = 1. \quad (21e)$$

Unfortunately, the above problem is still nonconvex since the objective function is fractional. However, we can apply bisection method to solve this problem. By introducing a new variable t , the optimization problem can be reformulated as

$$\max_{\mathbf{W}, t} \quad t, \quad (22a)$$

$$s.t. \quad Tr(\mathbf{Z}\mathbf{W}) \geq tN_i\sigma_i^2, \quad (22b)$$

$$Tr(\mathbf{N}_k\mathbf{W}) \leq P_k, \quad k = 1, 2, \dots, K, \quad (22c)$$

$$Tr(\mathbf{U}\mathbf{W}) \leq r_e N_w \sigma_w^2, \quad (22d)$$

$$Tr(\mathbf{V}_i\mathbf{W}) \geq r_i N_i \sigma_i^2, \quad i = 1, 2, \dots, K, i \neq w, \quad (22e)$$

$$\mathbf{W} \succeq 0, rank(\mathbf{W}) = 1, \quad (22f)$$

where

$$\mathbf{Z} = \mathbf{A} - t\mathbf{B} \quad (23)$$

$$\mathbf{U} = \mathbf{C} - r_e \mathbf{D} \quad (24)$$

$$\mathbf{V}_i = \mathbf{E}_i - r_i \mathbf{M}_i \quad (25)$$

It should be noticed that the rank-1 constraint violates the problem's convexity. Thus, by omitting the rank constraint and fixing the value of t , the problem turns into a convex form, specifically, a semidefinite programming (SDP) problem. Then, we can utilize bisection algorithm to solve (23) as shown in Algorithm. 1. To solve problem (23) we used CVX, a package for specifying and solving convex programs [10].

Algorithm 1 Bisection algorithm for solving (23).

1: Initialization:

Set t_{min} , t_{max} , n , η and N_{max} which correspond the lower bound of bisection searching range, the upper bound of bisection searching range, iteration number counting, accuracy of bisection algorithm and the maximum iteration number.

Compute \mathbf{N}_k , \mathbf{Z} , \mathbf{U} and \mathbf{V}_i using (20), (23), (24) and (25), respectively.

2: Iteration:

a) $t = (t_{min} + t_{max})/2$

b) Compute \mathbf{W} in (23) using CVX.

c) If step b) is feasible, $t_{min} = t$; Otherwise, $t_{max} = t$.

3: Termination:

The algorithm terminates either when $t_{max} - t_{min} \leq \eta$, or when $n \geq N_{max}$, where η is a predefined threshold and N_{max} is the maximum iteration number;

Output $\mathbf{W}_k^{opt} = \mathbf{W}_k^{(n)}$

Else, $n = n + 1$, and go to step 2).

Let us denote $\tilde{\mathbf{W}}$ as the solution obtained from CVX. If $rank(\tilde{\mathbf{W}}) = 1$, then we can use eigenvalue decomposition to obtain the optimal \mathbf{f}^{opt} ; Otherwise, randomization technique can be applied to obtain the \mathbf{f}^{opt} [11]. Specifically, we generate a set of random vectors which conform the Gaussian distribution $\mathcal{N}(\mathbf{0}, \tilde{\mathbf{W}}^{opt})$. Among these vectors, we select the ones that do not violate the constraints of (23) as the candidates and record their corresponding values of objective function (23a). Finally, the candidate vector that can achieve the maximum values of objective function (23a) can be viewed as a quasi-optimal solution.

IV. JOINT PRECODING DESIGN WITHOUT PRE-KNOWN WIRETAPPING KNOWLEDGE

In this section, we will consider the scenario where we do not know which user will be wiretapped. Therefore, we can not express the capacity achieved by eavesdropper as well as the wiretapped user's. Traditional algorithm that dealing with such circumstance might apply the leakage-based precoding (SLNR) scheme [12], which mainly minimizes the power that leaking to other user's channel space. We will compare our algorithm with SLNR algorithm in section V. In this paper, we attempt to constrain the power of all user's messages received by the eavesdropper within a fixed range.

$$\sum_{k=1}^K \|\mathbf{H}_{ek}\mathbf{F}_k\|^2 \leq P_{th}, i = 1, 2, \dots, K, \quad (26)$$

where P_{th} is the maximum efficient power received by eavesdropper that can be tolerated. Although we have no information about the wiretapped user, we can still execute a global optimization process that can greatly confine the eavesdropper's performance. That is, we attempt to maximize the minimum SINR of all the serving users while maintaining the individual transmitter's power constraints as well as the receiving power constraint of eavesdropper. Therefore, the

optimization problem can be formulated as

$$\max_{\mathbf{F}_k, k \in \{1, 2, \dots, K\}} \min_{i \in \{1, 2, \dots, K\}} \frac{\|\mathbf{H}_{ii}\mathbf{F}_i\|^2}{\sum_{k=1, k \neq i}^K \|\mathbf{H}_{ik}\mathbf{F}_k\|^2 + N_i \sigma_i^2}, \quad (27a)$$

$$s.t. \quad Tr(\mathbf{F}_k \mathbf{F}_k^H) \leq P_k, \quad k = 1, 2, \dots, K, \quad (27b)$$

$$\sum_{k=1}^K \|\mathbf{H}_{ek}\mathbf{F}_k\|^2 \leq P_{th}, i = 1, 2, \dots, K. \quad (27c)$$

By introducing a new variable z , the problem can be rewritten as

$$\max_{\mathbf{F}_k, z} \quad z, \quad (28a)$$

$$s.t. \quad Tr(\mathbf{F}_k \mathbf{F}_k^H) \leq P_k, \quad , k = 1, 2, \dots, K, \quad (28b)$$

$$\sum_{k=1}^K \|\mathbf{H}_{ek}\mathbf{F}_k\|^2 \leq P_{th} \quad (28c)$$

$$\frac{\|\mathbf{H}_{ii}\mathbf{F}_i\|^2}{\sum_{k=1, k \neq i}^K \|\mathbf{H}_{ik}\mathbf{F}_k\|^2 + N_i \sigma_i^2} \geq z, i = 1, 2, \dots, K. \quad (28d)$$

Using the same technique as in (10), (28c) can be expressed as

$$\sum_{k=1}^K \|\mathbf{H}_{ek}\mathbf{F}_k\|^2 = Tr(\mathbf{Q} \mathbf{f} \mathbf{f}^H) \leq P_{th}, \quad (29)$$

where

$$\mathbf{Q} = \mathbf{T}_f^H \left(\sum_{k=1}^K (\mathbf{P}_k^T \mathbf{P}_k)^T \otimes (\mathbf{P}_k^T \mathbf{H}_{ek}^H \mathbf{H}_{ek} \mathbf{P}_k) \right) \mathbf{T}_f \quad (30)$$

Similarly, (28d) can be written as

$$Tr(\mathbf{L}_i \mathbf{f} \mathbf{f}^H) \geq z N_i \sigma_i^2, i = 1, 2, \dots, K, \quad (31)$$

where

$$\mathbf{L}_i = \mathbf{E}_i - z \mathbf{M}_i \quad (32)$$

Similar to last section, we introduce $\mathbf{W} = \mathbf{f} \mathbf{f}^H$ with additional rank and semidefinite constraints. Drop the rank-1 constraint, the problem can be turned into a convex form, which is

$$\max_{\mathbf{W}, z} \quad z, \quad (33a)$$

$$s.t. \quad Tr(\mathbf{N}_k \mathbf{W}) \leq P_k, k = 1, 2, \dots, K, \quad (33b)$$

$$Tr(\mathbf{Q} \mathbf{W}) \leq P_{th} \quad (33c)$$

$$Tr(\mathbf{L}_i \mathbf{W}) \geq z N_i \sigma_i^2, i = 1, 2, \dots, K, \quad (33d)$$

$$\mathbf{W} \succeq 0 \quad (33e)$$

However, joint optimization \mathbf{W} and z is difficult, due to the nonconvex property brought by bilinear expression of \mathbf{L}_i [9]. Fortunately, the optimization problem (33) is in form of quasi-convex and bisection algorithm can still be applied here. Specifically, by fixing the value of z , the problem turns to optimize \mathbf{W} which is in a standard form of convex SDP and it can be solved here efficiently by software CVX. The bisection algorithm applied is similar to algorithm 1. The only difference is that instead of calculating \mathbf{Z} , \mathbf{U} and \mathbf{V}_i , we need to calculate \mathbf{Q} and \mathbf{L}_i . Similar to (22), if $rank(\mathbf{W}^{opt}) = 1$, we use eigenvalue decomposition to obtain the optimal \mathbf{f}^{opt} ; Otherwise, we resort to randomization technique.

V. NUMERICAL RESULTS AND DISCUSSIONS

Numerical results are demonstrated in this section so as to verify the effectiveness of our proposed method. For simplicity of expression, we use a vector $[N_1 \ N_2, \dots, N_K]$ to denote the antenna number equipped in each cell. For instance, [2 2] represents that we have two cells and each cell involves a dual-antenna base station and a dual-antenna user. In all the simulations, we assume $w = 1$ which means the first user will always be wiretapped by the eavesdropper. Moreover, we let $\sigma_i^2 = \sigma_e^2 = \sigma_s^2 = \sigma^2$ and $P_k = P, k = 1, 2, \dots, K$. Therefore, the SNR is defined as $\frac{P}{\sigma^2}$. The simulation results are the averaged data over 1000 channel realization.

Firstly, we investigate the wiretapped user's capacity versus the thresholds of r_e . We investigate two types of antenna configuration, which are [4 4] and [4 4 4]. It can be observed from Fig. 2 that the wiretapped user's capacity grows with the increase of r_e under both antenna configurations. Increasing r_e will lead to a larger feasible set for the problem (8) and naturally it will achieve a better result for the wiretapped user's capacity. Similar analysis also works for the value of r_i . With fixed r_e , increasing r_i leads to less feasible set. Therefore, a lower wiretapped user's capacity is expected for a larger r_i . Moreover, it shows that with the same values of r_e and r_i [4 4] always achieves better performance than [4 4 4] since an additional transmitter will bring more interference.

Then, we examine the secrecy capacity achieved by our two algorithms and compare them with traditional SLNR method. Similarly, we execute our simulation under the antenna configurations [4 4] and [4 4 4]. With prefixed value of $r_i = r_e = 1$ and $P_{th} = 20$ dB, we compare the performances of these three algorithms versus SNR. From Fig. 3 we see that our two algorithms outperform the existing SLNR based precoding method. Besides, for the fixed r_e , our algorithm with pre-known wiretapping knowledge outperforms the one without pre-known wiretapping knowledge, which demonstrates the importance of pre-known wiretapping knowledge.

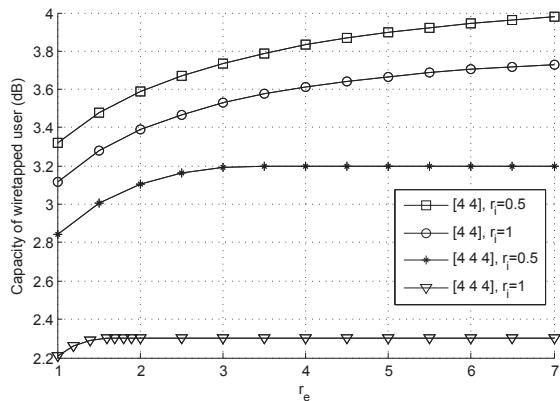


Fig. 2. Capacity of wiretapped user versus r_e for the cases of [4 4] and [4 4 4].

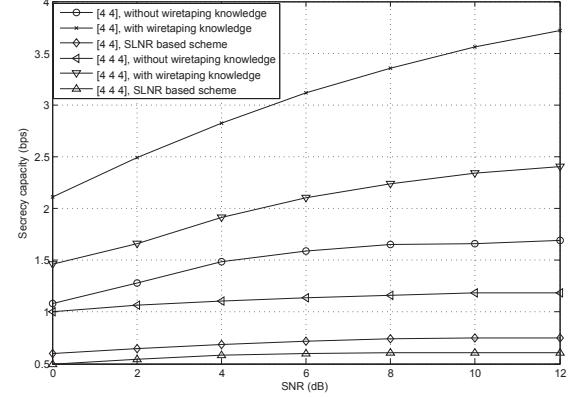


Fig. 3. Performance comparisons between our proposed algorithms and SLNR based scheme for the cases of [4 4] and [4 4 4].

VI. CONCLUSION

This paper considers the precoding designs in CoMP system with and without the wiretapping knowledge, respectively. Simulation results verify the effectiveness of our proposed algorithms. Though this paper assumes that all the CSI is perfect, perfect CSI is difficult to acquire in practical scenario. Therefore, in our following studies, we will concentrate on the secrecy studies based on imperfect CSI.

REFERENCES

- C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 29, pp. 656-715, 1949.
- A. Wyner, "The Wire-Tap Channel," *Bell Sys. Tech. J.*, pp. 1355-1387, Oct. 1975.
- C. Jeong, I. Kim and D. Kim, "Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System," *Signal Processing, IEEE Transactions on*, vol. 60, no. 1, pp. 310-325, Jan. 2012.
- S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.
- J. Huang and A. Swindlehurst, "QoS-constrained robust beamforming in MISO wiretap channels with a helper," *Signals, Systems and Computers (ASILOMAR), 2011 Conference Record of the Forty Fifth Asilomar Conference on*, pp. 188-192, Nov. 2011.
- H. Shen, B. Li, M. Tao and X. Wang, "MSE-based transceiver designs for the MIMO interference channel", *Wireless Communications, IEEE Transactions on*, vol. 9, no. 11, pp. 3480-3489, Nov. 2010.
- M. Fadel, A. El-Keyi and A. Sultan, "QoS-Constrained Multiuser Peer-to-Peer Amplify-and-Forward Relay Beamforming," *Signal Processing, IEEE Transactions on*, vol. 60, no. 3, pp. 1397-1408, Mar. 2012.
- R. Horn and C. Johnson, *Matrix Analysis*, Cambridge, U.K.: Cambridge Univ. Press, 1985.
- S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
- CVX Research, Inc. CVX: Matlab software for disciplined convex programming, version 2.0 beta. <http://cvxr.com/cvx>, September 2012.
- Y. Huang and D. Palomar, "Rank-Constrained Separable Semidefinite Programming With Applications to Optimal Beamforming," *Signal Processing, IEEE Transactions on*, vol. 58, no. 2, pp. 664-678, Feb. 2010.
- M. Sadek, A. Tarighat, and A. Sayed, "A leakage-based precoding scheme for downlink multi-user MIMO channels," *Wireless Communications, IEEE Transactions on*, vol. 6, no. 5, pp. 1711-1721, May 2007.